ST LAWRENCE CHURCH OF ENGLAND PRIMARY SCHOOL

E-Safety Policy

E-Safety Policy

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at St Lawrence Church of England Primary School we build in the use of these technologies in order to arm our children with the skills to access life-long learning and employment.

Computing covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of computing within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Blogs and Wikis
- Podcasting
- Multimedia
- Gaming
- Mobile devices

Whilst exciting and beneficial both in and out of the context of education, much computing, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At St Lawrence we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement are inclusive of fixed and mobile internet technologies provided by the school.

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the head teacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The head teacher is the named e-safety co-ordinator at St Lawrence.

This policy, supported by the school’s acceptable use agreement, is to protect the interests and safety of the whole school community. It is linked to the following school policies: child protection, safeguarding positive relationships and behaviour, health and safety, anti-bullying and PHSE.

Managing the school e-safety messages

We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used. These messages will be appropriate to the age of the children being taught. E-safety messages will be displayed in the classrooms and communicated to our parents through letters and in the school newsletter.

E-safety in the Curriculum

The school provides opportunities within a range of curriculum areas to teach about e-safety.

Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-safety curriculum.

The teaching of e-saftey focuses on helping children to recognise inappropriate content, conduct, contact and commercialism and helps them learn how to respond or react appropriately.

Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues.

Pupils know how to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.

Security, Data and Confidentiality

Staff may, in some circumstances, use cloud based storage, which is password protected to store and access information conveniently.

Staff should be aware of their responsibilities when accessing sensitive school data:

School data will only be accessed by staff, using their own username and password.

School data will not be duplicated onto personally owned equipment.

Portable devices are encrypted and data can only be accessed using a secure log in.

Managing the Internet

All use of the the school internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

In school children will have supervised access to Internet resources (where reasonable) through the school’s fixed and mobile internet technology.

Filters are set to support ‘safe searches’ in school, the filters are used to manage any internet research. No filter makes an internet search 100% safe, it is important that all users are aware of this.

If Internet research is set for homework, staff will remind students of their e-safety training. Parents are encouraged to support and supervise any further research.

Infrastructure

St Lawrence Church of England Primary has a contract with the Local Authority, who provide our broadband services.

Our school has the facility for additional web filtering (cachepilot) which is the responsibility of the e-safety co-ordinator and ICT administrators. The ICT administrators regularly check for updated / improved solutions to monitoring and filtering internet use within school.

St Lawrence Church of England Primary is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

If staff or pupils discover an unsuitable site, the incident should be reported immediately to the teacher and then passed on to the e-safety coordinator.

If there are any issues related to viruses or anti-virus software, the e-safety co-ordinator and ICT administrator should be informed.

Mobile Technologies

Personal Mobile devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use during designated times. These are not to be used at any time whilst children are present.

The school is not responsible for the loss, damage or theft of any personal mobile device.

Managing email

The use of email within school is an essential means of communication for staff.

Pupils currently do not have access to individual email accounts.

Staff must use the schools approved email system for any school business.

Staff must inform (the esafety co-ordinator/ line manager) if they receive an offensive or inappropriate e-mail.

Pupils may be introduced to email as part of the Computing Scheme of Work.

Social Networking

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day.

The school also strongly discourages children from using age inappropriate social networking outside of school. Should the staff be made aware of incidents or activities on these social networks, which has a direct effect on the children's behaviour or attitudes within school, then the school reserves the right to take action regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

Safe Use of Images

Taking of Images and Film

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes field trips. School's own mobile devices must be used in this case.

Publishing pupil's images and work

All parents/guardians will be asked to give permission to use their child's work/photos in publicity materials or on the school website.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.

Parents/ carers may withdraw permission, in writing, at any time.

Storage of Images

Images/ films of children are stored securely on the school server and / or teacher's individual school laptops.

Misuse and Infringements

Complaints

Complaints or concerns relating to e-safety should be made to the e-safety coordinator.

Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-safety coordinator.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA. Staff are aware that misuse or misconduct could lead to disciplinary action.

Equal Opportunities

Pupils with additional needs

The school endeavours to deliver a consistent message to parents and pupils with regard to the schools' e-safety rules.

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety.

Internet activities are planned and well-managed for these children.